The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image

Soo Ann Nie[1], Ghazali Sulong[2], Rozniza Ali[3], Andrew Abel[4]
[1]Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
[2,3]School of Informatic and Applied Mathematics, Universiti Malaysia Terengganu, Malaysia
[4]Xi'an Jiaotong-Liverpool University, China

Article Info

Article history:

Received Dec 3, 2018
Revised Apr 18, 2019
Accepted Jun 10, 2019

Keywords:

Chi square
Cover image
Knight tour
Least significant bit
Steganography

ABSTRACT

Steganography is one of the method to communicate in a hidden way. In another word, steganography literally means the practice of hiding messages or information within another data. Previous studies have proposed various steganography techniques using different approaches including Least Significant Bit (LSB), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). However, different approaches still have its own weaknesses. Therefore image stenography using Knight Tour Algorithm with Least Significant Bit (LSB) technique is presented. The main objective is to improve the security factor in the stego image. Basically, the proposed technique is divided into two parts which are the sender and receiver side. Then, steganalysis which is a type of attack on stenography algorithm is used to detect the secret message in the cover image by the statistical analysis of pixel values. Chi Square Statistical Attach which is one of the type of steganalysis is used to detect these near-equal Po Vs in images and bases the probability of embedding on how close to equal the even pixel values and their corresponding odd pixel values are in the test image. The Knight Tour Algorithm is applied due to the common Least Significant Bit technique that is weak in security and easily decoded by outsider.

Corresponding Author:

Rozniza Ali,
School of Informatic and Applied Mathematics,
Universiti Malaysia Terengganu,
21030 Terengganu, Malaysia.
Email: rozniza@umt.edu.my

1. INTRODUCTION

With the rise of modern technology, it is very easy to distribute digital media, such as audio, images and videos, online. This leads to several problems as it is very easy for personal information to be leaked to other people. This means that toprevent leaked data, there is a dramatic increase in demand for methods to protect confidential data. Presently, there are few effective techniques developed and available in the market to provide the security to hide confidential data from public and still be able to pass the data to the correct person. One of the methods to protect from unauthorized access and use is steganography.

Steganography refers to the practice of hiding messages or information within other data. According to Laskar and Hemachandran [1], the goal of steganography is to hide messages inside other "harmless" digital media in a way that does not allow any person to even detect the presence of a secret message. Johnson and Jajodia [2] also state that the main goal of steganography is to communicate securely in such a way as to avoid drawing suspicion to the transmission of hidden data. Steganography is divided mainly into three categories which are image steganography, audio steganography and video steganography. This paper introduces a new approach for image steganography on a non-encrypted images that combines the widely used Least Significant Bit (LSB) technique with the Knight Tour Algorithm.

2. BACKGROUND

Encrypting data and embedding a secret message in an image is a real challenge. There are many established techniques, such as watermarking and steganography, for transmitting the data within images safely. Steganography is also capable of preventing secret messages being used illegally by unauthorized people.

According to Johnson and Jajodia [2], steganography does not alter the structure of the secret message, but hides it inside a medium so that the change is not visible. "In other words, steganography prevents an unintended recipient from suspecting that the data exists and the security of the steganography system relies on secrecy of the data encoding system Conway [3]".

Image steganography techniques can be classified into two major categories, spatial domain techniques and frequency domain techniques. In spatial domain techniques, image pixels are manipulated to store the secret message, while in frequency domain techniques, the image is first transformed by applying a transformation like a discrete wavelet transform, and then an embedding technique is applied to hide the message. Both techniques have their own advantages and disadvantages. In the spatial domain, there are a number of different categories, including Least Significant Bit steganography, pixel value differencing steganography, mapping based steganography, and palette based steganography [4]. In this paper, the Least Significant Bit (LSB) technique will be used for image steganography. The LSB technique embeds secret messages into the cover image by replacing the least significant bits directly.

However, once the encoding system is known, the steganography system is easily defeated. Therefore, the defence of the chosen steganography technique against various attacks from any adversary is very important. The performance of various steganography methods can be evaluated by two of the most important parameters [5], which are the robustness and security of the stego image.

The security factor refers to the secret data being hidden even after being targeted by various attacks. If the secret message is visible in the cover image, its file format, or is discovered during steganalysis, this proves that steganography is a failure. Robustness represents the amount of distortion that a digital cover can endure to keep the secret message safe. This factor includes ensuring the unity of the secret message for the receiver even if the stego image is damaged by any attacks during the transmission phase. Therefore, the purpose of technique proposed in this paper is to achieve and at the same time improve the robustness and security of the stego image. The aim is that both the host image and the stego image cannot be differentiated by any differences after undergoing Chi-square statistical attack, and the secret message remains in its original form.

A number of techniques that have been proposed using the LSB method. Zhang and Tang [6] proposed an enhancement over Least Significant Bit (LSB) technique that selects random sets of pixels with the help of a pseudo random number and then embeds *n* bits in each pixel using addition and modular division operations. The length of the bit stream of the embedded message affects the *n* value. Both security and capacity are addressed.

Additionally, Mathkour *et al*. [7] proposed a spiral based LSB substitution approach for hiding messages in images. This approach is based on LSB substitution technique applied to RGB colour components of an image. The image is divided into many image segments and different processing is applied to each segment.

In this paper we propose to combine the Knight's Tour Algorithm with the LSB technique to enhance the steganography method. In the Knight's Tour Algorithm, the image is considered just like a surface of a chessboard. According to Sobol and Levitan [8], the advantages of the Knight's Tour method over the Pseudo-Random Number Generator (PRNG) technique are that it is a self-developed algorithm based on the Knight's Tour mathematical problem, and it is almost undetectable by unintended or unauthorised receivers.

As discussed previously, it is important that the steganography image is not vulnerable to various attacks and the secret message conveying is not visible to anyone. However, many previous studies [9, 10] have identified that steganography techniques do not successfully hide the secret message in the stego image [11]. In this paper, the Chi-square statistical attack is used to test whether the existence of the secret message in the stego image can be easily detected.

3. PROPOSED FRAMEWORK

In this paper, we propose a new approach to achieve higher security by using the LSB method with Knight Tour Algorithm. The two main stages are the embedding stage for the cover image, and the receiving stage for the stego image.

3.1. Least significant bit (LSB)

Least Significant Bit (LSB) insertion is one of the most popular techniques in the spatial-domain category. It is a common and simple approach to embed a secret message in a host image. The LSB technique works by using the least significant bits of each pixel in one image to hide the most significant bits of another [18]. Changing the LSB of a pixel will cause some small changes in pixel intensity, however, these changes cannot be identified by the human eye [2]. In the receiving stage, the data will be extracted and decompressed. The cipher text is then decrypted to reveal the embedded message. Figure 1 illustrates the entire general framework process for sender and receiver.

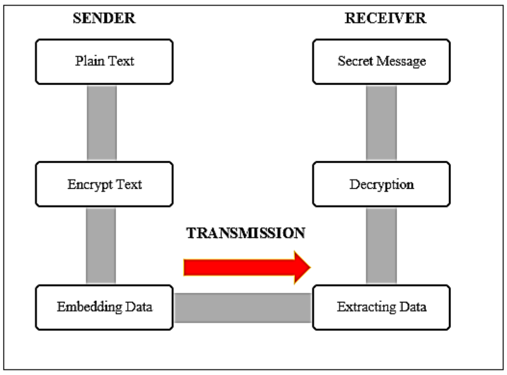

Figure 1. General stage for sender and receiver

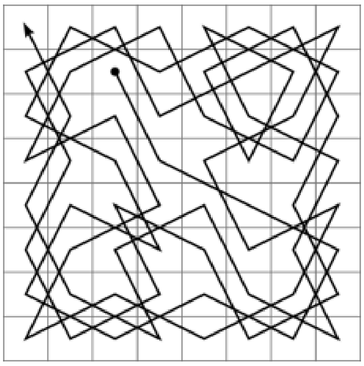

Figure 2. Knight's movement on a board

3.2. Knight tour algorithm

The “Knight Tour” algorithm was first analysed by Euler in 1759, and is a suitable technique to formulate the sequence of the secret bit stream within the image pixels. The Knight Tour algorithm is a self-developed algorithm based on the knight tour mathematical problem [6]. It has the advantage over the Pseudo Random Number Generator (PRNG) technique in that it cannot be identified by unintended receivers. The Knight Tour Algorithm divides the chess board into blocks. In the n × n chessboard, the knight travels to all squares once, as shown in Figure 2. By using this idea, high security can be achieved in steganography since the search space will be significantly high whether or not the the starting square of the knight’s move is known [13].

- Sender side: First of all, the plain text has to be prepared beforehand. The plain text is encrypted and converted to binary form from its original ASCII value. The image pixels will be used to embed the encrypted message. From here, LSB is used to embed the secret message together with the cover image by replacing the least significant bit of pixel values with the encrypted information bits. Thus, a stego image is created. The entire process is illustrated in Figure 3.
- Receiver side: The stego image is then transmitted to the receiver. The receiver receives the stego key and the extracting algorithm to decode the image. The pixel binary values are used with the LSB decoder to separate the encrypted data from the image pixel values. The extracting algorithm is used to decrypt the data to reveal the hidden message. The process is shown in Figure 4.
- Embeddeding stage: The embedding stage, shown in Figure 5 is the most important part of the process. This determines which order the image pixels will be altered with the secret message. The order of pixels to be changed is determined by using the Knight Tour Algorithm [14]. This provides higher security to the embedded data as only the sender and receiver can determine the location of its initial chosen pixel and the later paths correctly, in comparison to the Pseudo Random Number Generator (PRNG) technique. The LSB technique is then used to embed the message into the cover image. Finally a stego image is created.

3.3. Applying knight tour algorithm

The Knight Tour Algorithm firstly divides the chess board into 4x4 blocks. Four groups of the four squares in each block are named “Right Diamond”, “Left Diamond”, “Right Square” and “Left Square” as shown in Figure 6 [13].

The algorithm will cover all pixels if the size of the image is divisible by 4. However, extra columns or rows which are less than 4 will be unusable. The proposed algorithm has the following steps:

a. Divide the image’s width and height by four by ignoring the extra pixels.
b. Divide the image into 4x4 pixel blocks.

c. Start from the pixel indicated by the stego-key, and after that start with one group of the same till all pixels in that group are traversed.
d. All 4 squares must be traversed to move from one block to the next block.
e. After the movement of the group of colour has finished, move on with the next group of colours.
f. Repeat all the steps above to traverse all the pixels in the image.

After the series of certain pixels has been determined in the steps above, the LSB technique is used to substitute the image pixels with the bit stream of the secret message.

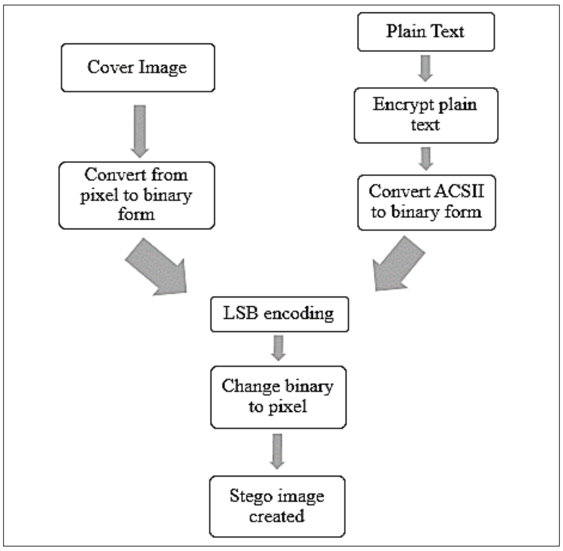

Figure 3. Sender side proposed process

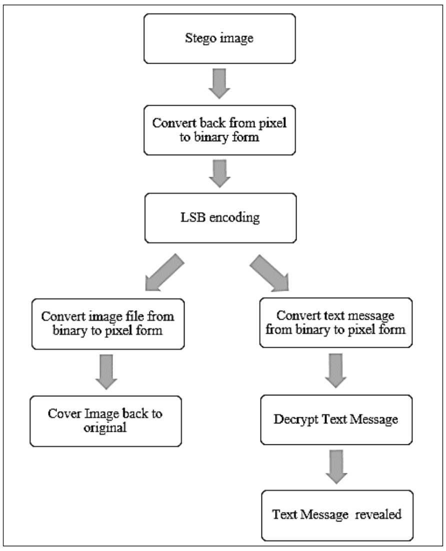
Stego image
Convert back from pixel to binary form
LSB encoding
Convert image file from binary to pixel form
Convert text message from binary to pixel form
Cover Image back to original
Decrypt Text Message
Text Message revealed

Figure 4. Receiver side proposed process

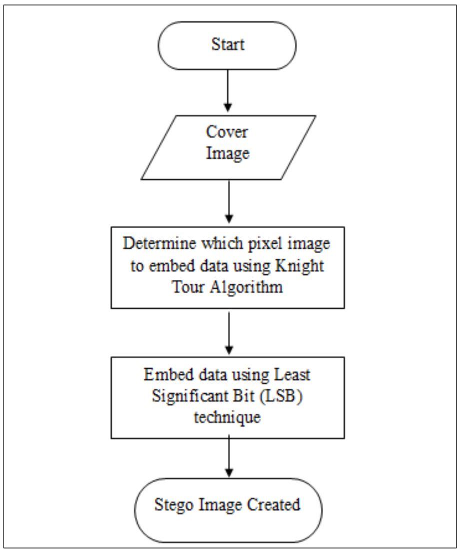
Start
Cover Image
Determine which pixel image to embed data using Knight Tour Algorithm
Embed data using Least Significant Bit (LSB) technique
Stego Image Created

Figure 5. Embedding stage

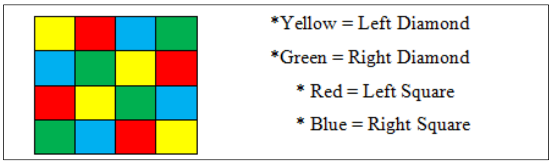

Figure 6. Four groups of squares representing block of pixels

3.4. Applying LSB

The LSB technique works by changing the least significant bit, in a greyscale image, generally the eighth bit, to a bit of the secret message. An 800×600 pixel image can theoretically store up to 1,440,000 bits or 180,000 bytes of embedded data [21]. An 8-bit grayscale image also needs 8 pixels for the embedding process. The LSB embedding technique is described as below:

a. Read the cover image in binary, identifying dimensions.
b. Use Knight Tour Algorithm to obtain pixels to hide information in the cover image.
c. Apply LSB technique by changing the eighth bit on every chosen 8 bit pixel to hide information, leaving the most significant bits (MSB) unchanged. The algorithm that can be used to change the bit of a 8 bit image is:

```
$if\ pixel\ value = odd$
$Then\ increment\ by\ 1$
$Else\ if\ the\ pixel\ value = 255$
    $then\ decrement\ by\ 1$
$If\ pixel\ value = odd$
$if\ bit = 0$
    $then\ add\ 1$
            $else\ if\ the\ pixel\ value = 255$
    $if\ bit\ value = 0$
            $then\ decrement\ by\ 1$
$else\ if\ pixel\ value = even$
$if\ bit = 1$
    $then\ increment\ by\ 1$
```

d. Replace the LSB by one bit of the bits to be embedded.
e. Finally, the secret message is hidden using Bit Replcamenet method on the cover image.

3.5. Extraction stage

The final stage is the extraction by the receiver. Figure 7 illustrates the extraction stage.

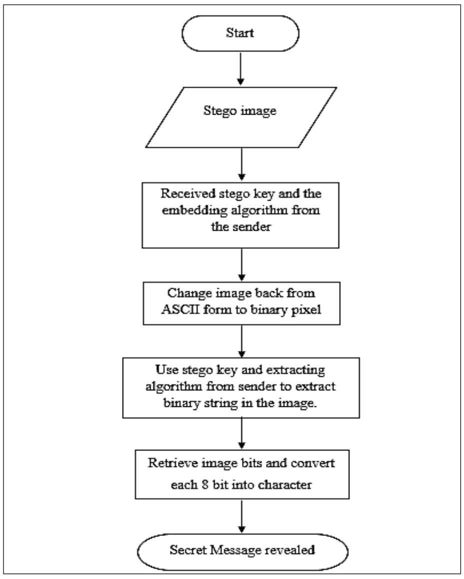
Start
Stego image
Received stego key and the embedding algorithm from the sender
Change image back from ASCII form to binary pixel
Use stego key and extracting algorithm from sender to extract binary string in the image.
Retrieve image bits and convert each 8 bit into character
Secret Message revealed

Figure 7. Extraction stage

4. RESULT AND DISCUSSIONS

This section presents the results of steganography technique and its effect on the cover image. The standard cover images used are Elaine.tiff and Stream.tiff. A plain text acting as the secret message will be hidden inside the cover image. Chi Square Statistical Attack will be used to evaluate the level of security of the cover image after it had undergo steganography.

4.1. Dataset

We use a standard dataset for the cover images. The cover image are being used in 8-bit grayscale mode for testing. Each image is 512x512 pixels in size. These images are taken from *http://sipi.usc.edu/database/database.php?volume=misc*. Figure 8 shows examples of the cover images used.

Figure 8. Cover image

4.2. Measurement and evaluation

The proposed algorithm will be evaluated based on several factors which are imperceptibility, robustness and security using Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) formulas, and Chi-Squared Statistical Attack. PSNR formula is calculated to evaluate the imperceptibility of the stego image while MSE is one of the formulas in PSNR. The higher the quality of the stego image, the higher the level of imperceptibility of the hidden secret message. On the other hand, Chi Square Statistical Attack is used to evaluate the level of security and robustness of the stego image.

4.3. Results

Figure 9 shows the comparison between the original Elaine image and the Elaine stego image after undergoing steganography. To the human eye, both images appear exactly the same. PSNR is used to measure image imperceptibility. A greater PSNR value will show a lower degree of image distortion by the embedding algorithm and the higher the quality of the stegpo image. After embedding, the PSNR should remain similar.

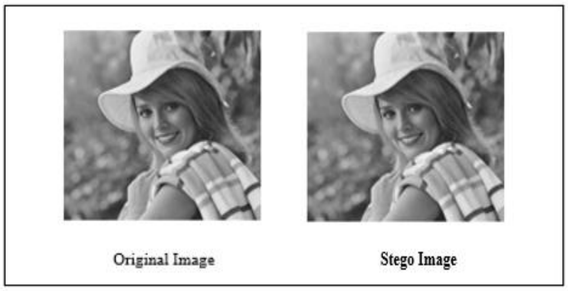

Figure 9. Original Elaine image and its stego image

Steganalysis is then conducted using Chi Square Statistical Attack. It is applied to images to check the likelihood of conveying a secret message. The attack is based on the distribution probability of zeros and ones over the image. Figure 10 illustrates the expected result of Chi Square attack on the stego image using simple LSB method only. Due to space limitations, we present some example results.

The results show in Figure 11, Figure 12 and Figure 13 that for the LSB method only, the existence of the message can be easily detected when the probability trend falls dramatically from around one (hundred percent) to zero. However, when our proposed approach is used for embedding data, the results are noticeably different. There are cases where the Chi-square diagram detects almost no embedded data in the stego images.

Conversely, the PSNR value of both techniques are almost the same. The deviation from zero are just visible in few points of probability trend and especially, these values are not even more than one percent. This is because the proposed method is still the using the same embedding technique.

The results clearly show that the security of the proposed technique is higher compared to the simple LSB method against Chi-square Statistical Attack. Overall, by comparing LSB method with our proposed LSB and Knight Tour Algorithm, the Knight Tour Algorithm increases the image security. To be able to decode the stego image, sender has to give the receiver the algorithm. LSB acts as a first layer of security while Knight Tour Algorithm acts as a second layer. Since LSB is a common method, it is easy for outsiders to detect and extract the data from the image. However, together with Knight Tour Algorithm, although the outsider may be able to extract the data from the image, they would not be able to re-assemble the original message due to its unpredictable data embedding.

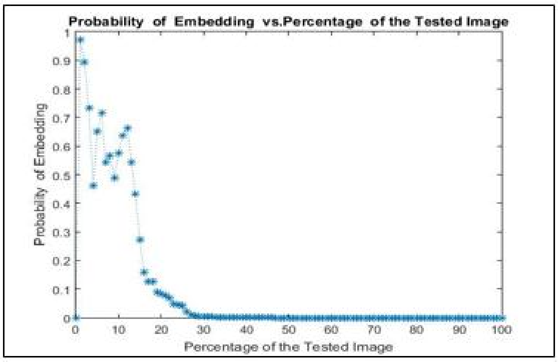

Figure 10. Chi-square result of LSB method for embedding 15kb data-stream

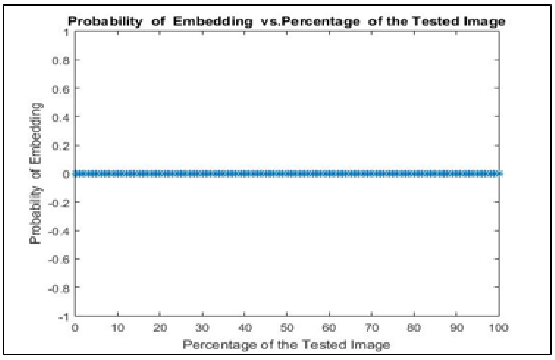

Figure 11. Chi-square result of LSB with knight tour algorithm method for embedding 15kb data-stream

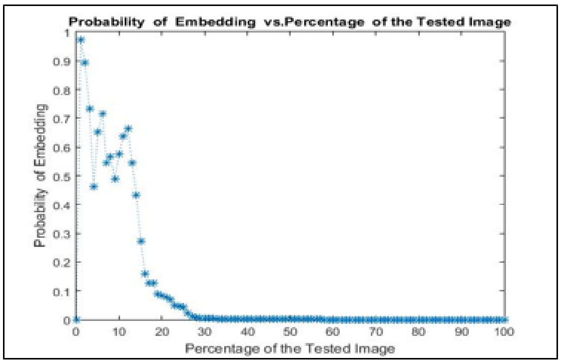

Figure 12. Chi-square result of LSB method for embedding 25kb data -stream

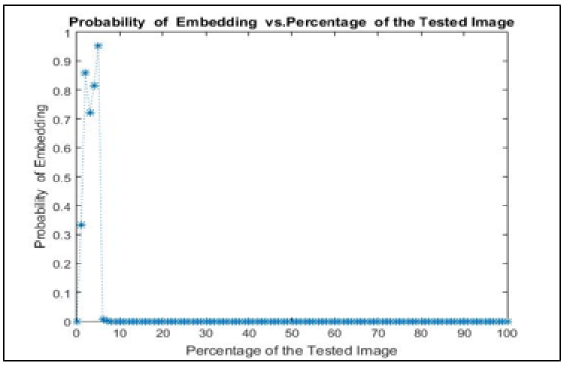

Figure 13. Chi-square result of LSB with knight tour algorithm method for embedding 25kb data-stream

5. CONCLUSION

This study proposed an enhanced technique to the existing common LSB technique combined with the Knight Tour Algorithm. Widely used grayscale images were was chosen to test the proposed technique. We considered the security and the robustness of the stego image. However, Knight Tour Algorithm has a fatal flaw in the size of image that can be used as cover. Only image size that can divided by 4 without any remainder enables the algorithm to be able to walk through the whole image pixels for encoding. Therefore, for future work, to enable the algorithm to be used in any size as cover image. Also, add in another steganography technique to increase capacity of embedding in the cover image as it can covers maximum up to 32.765KB data size due to limited space is available.

ACKNOWLEDGEMENTS

Gratefully acknowledges the collaboration work between Universiti Teknologi Malaysia and Universiti Malaysia Terengganu.

REFERENCES

[1] S. A. Laskar and K. Hemachandran, “An anlysis of stenography and steganalysis technique,” *Assam University Journal of Science and Technology*, vol. 9, no. 2, pp. 83-103, 2012.

[2] N. F. Johnson, *at al.*, “Exploring stenganography: Seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26-34, 1998.

[3] M. Conway, “Code Wars: Steganography, Signal Intelligence, and Terrorism,” *Knowledge Technology & Policy*, vol. 16, no. 2, pp. 45-62, 2003.

[4] G. Swain and S. Lenka, “Steganography using two sided, three sided and four sided match methods,” *International Journal of Computer Science & Engineering Technology*, vol. 1, no. 2, pp. 127-33, 2013.

[5] P. Rai, S. Gurung e M. K. Ghose, “Analysis of image steganography techniques: A survey,” Computer Applications, pp. 11-17, 2015.

[6] H. J. Zhang and H. J. Tang, “A novel image steganography algorithm against statistical analysis,” em Machine Learning and Cybernatics, 2007.

[7] H. Mathkour, G. M. R. Assassa, A. A. Muharib and I. Kiady, “A novel approach for hiding messages in images,” *em Singal Acquisition and Processing*, 2009.

[8] I. M. Sobol and Y. L. Levitan, “A pseudo-random number generator for personal computers,” *Computer & amp: Mathematics with Applications*, vol. 37, pp. 33-40, 1999.

[9] N. Provos, *at al.*, “Hide and Seek: An Introduction to steganography,” *IEEE Security & Privacy*, vol. 1, no. 3, 2003.

[10] M. Bashardoost, G. Sulong and P. Gerami, “Enhances LSB image stegaography by using Knight Tour Algorithm,” *Computer Science Issue*, vol. 10, no. 2, 2013.

[11] K. Rabah, “Steganography - The art of hiding data,” *Information Technology*, vol. 3, no. 3, pp. 245-269, 2004.

[12] H. Chun-Hsiang, C. Shang-Chih and W. Ja-Ling, “Digital-invisible ink data hiding based on spread spectrum and quantization techniques,” *Transaction on Multimedia*, vol. 10, no. 4, 2008.

[13] V. Thanikaiselvan, P. Arulmozhivarman and A. Rengarajan, “Horse riding & hiding in image for data guarding,” *Procedia Engineering*, vol. 30, pp. 36-44, 2012.

[14] I. Parberry, “An efficient algorithm for the Knight's tour problem,” *Discrete Application Mathematics*, vol. 73, pp. 251-260, 1997.

[15] V. L. Reddy, D. A. Subramanyam and D. P. Chenna Reddy, “Implementation of LSB steganography and its evaluation for various file formats,” *Advanced Networking and Applications*, vol. 2, no. 5, pp. 868-872, 2011.

[16] A. A.-A. Gutub, “Pixel indicator technique for RGB image steganogrphy,” *Emerging Techologies in Web Intelligence*, vol. 2, no. 1, 2010.

[17] C. Kraetzer, J. Dittmann and L. Lang, “Transparency benchmarking on audio watermarks and steganography,” *Security, Steganography, and Watermarking of Multimedia Contents*, pp. 60721J-21-60721J-13, 2006.

[18] Z. Xinpeng and W. Shuozhong, “Vulnerability of pixel-value differencing steganography of histogram analysis and modification for enhanced security,” *Pattern Recognition Letters*, vol. 25, no. 3, pp. 331-339, 2004.

[19] A. H. Tariq, A. Q. Mahmoud and B. Hassan, “A testbed for evaluating security and robustness of steganogrphy techniques,” *IEEE 46th Midwest Symposium on Circuits and Systems*, vol. 3, pp. 1583-1586, 2003.

[20] M. Douglas, K. Bailey and M. Leeney, “An overview of steganography techniques applied to the protection of biometric data,” *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333-17373, 2018.

[21] H. Maulana and E. R. Syahputra, “Analysis of multiple data hiding combined coloured visual crytography and LSB,” *Information and Communication Technology*, 2017.

[22] D. Maltoni and R. Cappelli, “Advances in Fingerprint Modeling,” *Image and Vision Computing*, vol. 27, no. 3, pp. 258-268, 2009.

[23] W. C, T. S and G. V, “Image quality measures for fingerprint image enhancement,” *Multimedia Content Representation, Classification and Security, Springer,* Berlin Heidelberg, pp. 215-222, 2006.

[24] R. R and H. K, “A review on image enhancement of fingerprint using directional filters,” *Assam University, Journal of Science and Technology*, vol. 7, no. 2, pp. 52-57, 2011.

[25] B. M. A and G. S. H, “Systematic methods for the computation of the directional fields and singular points of fingerprints,” *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol. 24, no. 7, pp. 905-919, 2002.

[26] S. “An automatic fingerprint classification technique based on singular points and structure shape of orientation fields,” Fakulti Sains Komputer dan Sistem Maklumat, 2012.

[27] B. J. L, C. G. T, G. P. J, C. R and W. C. L, “Evaluation of pattern classifiers for fingerprint and OCR applications,” *Pattern Recognition*, vol. 27, no. 4, pp. 485-501, 1994.

[28] J. A. K, P. S and H. L, “A multichannel approach to fingerprint classification,” *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol. 21, no. 4, pp. 348-359, 1999.

[29] J. A. K, H. L, P. S and B. R, “An identity-authentication system using fingerprints,” *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1365-1388, 1997.

[30] C. A and G. S, “A fast fingerprint image enhancement algorithm using a parabolic mask,” *Computers and Electrical Engineering*, vol. 34, no. 3, pp. 250-256, 2008.

[31] H. L, W. Y and J. A, “Fingerprint image enhancement algorithm and performance evaluation,” *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol. 20, no. 8, pp. 777-789, 1998.

[32] H. M. F, “Contrast fingerprint enhancement based on histogram equalization followed by bit reduction of vector quantization,” *Computer Science and Network Security*, vol. 11, no. 5, pp. 116-123, 2011.

[33] F. M, H. J and X. J, “A novel fingerprint image preprocessing algorithm,” *Applied mechanics and materials*, vol. 347, pp. 2528-2532, 2013.

[34] K. J. S and K. E. K, “An enhanced thinning Algorithm using parallel processing,” *Image Processing*, vol. 3, pp. 452-455, 2001.

[35] Z. J, C. F and G. J, “A novel algorithm for detecting singular points from fingerprint images,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 31, no. 7, pp. 1239-1250, 2009.

[36] N. F. Johnson, *at al.*, “Exploring steganography: Seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26-34, 1998.

BIOGRAPHIES OF AUTHORS

Ann Nie Soo, Current Position: IT Consultant for Business Intelligence Software. Education: Msc. Computer Science (Uni. Teknologi Malaysia)

Ghazali Sulong, Current Position: Professor at Universiti Teknologi Malaysia. Education: Phd in Computer Science, Wales University. Specialization: Image Processing, Biometrics, Watermarking

Rozniza Ali, Current Position: Senior Lecturer, Universiti Malaysia Terengganu. Highest Education: PhD in Computer Science, Stirling University. Specialization: Machine Learning, Image Processing, Pattern Recognition

Andrew Abel, Current Position: Lecturer at Xi'an Jiaotong-Liverpool University. Highest Education: PhD in Computer Science, Stirling University. Specialization: Machine Learning, Artificial Intelligence